Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 4)
Which of the following is the PRIMARY accountability for a control owner?

A. Communicate risk to senior management.
B. Own the associated risk the control is mitigating.
C. Ensure the control operates effectively.
D. Identify and assess control weaknesses.

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

A. Escalate the non-cooperation to management
B. Exclude applicable controls from the assessment.
C. Review the supplier's contractual obligations.
D. Request risk acceptance from the business process owner.

Answer: C

NEW QUESTION 3
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

A. Recovery time objectives (RTOs)
B. Segregation of duties
C. Communication plan
D. Critical asset inventory

Answer: C

NEW QUESTION 4
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases
C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

A. Business impact analysis (BIA) results
B. Risk scenario ownership
C. Risk thresholds
D. Possible causes of materialized risk

Answer: C

NEW QUESTION 6
- (Exam Topic 4)
An organization has decided to implement a new Internet of Things (loT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

A. Develop new loT risk scenarios.
B. Implement loT device monitoring software.
C. Introduce controls to the new threat environment.
D. Engage external security reviews.

Answer: A

NEW QUESTION 7
- (Exam Topic 4)
Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?

A. IT security manager
B. IT personnel
C. Data custodian

D. Data owner

Answer: D

NEW QUESTION 8
- (Exam Topic 4)
Which of the following would provide the BEST evidence of an effective internal control environment/?

A. Risk assessment results
B. Adherence to governing policies
C. Regular stakeholder briefings
D. Independent audit results

Answer: D

NEW QUESTION 9
- (Exam Topic 4)
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

A. Recommend risk remediation
B. Change the level of risk appetite
C. Document formal acceptance of the risk
D. Reject the business initiative

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

A. The cost associated with incident response activitiesThe composition and number of records in the information asset
B. The maximum levels of applicable regulatory fines
C. The length of time between identification and containment of the incident

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.

Answer: C

NEW QUESTION 12
- (Exam Topic 4)
Which of the following is the MOST important consideration when developing risk strategies?

A. Organization's industry sector
B. Long-term organizational goals
C. Concerns of the business process owners
D. History of risk events

Answer: B

NEW QUESTION 13
- (Exam Topic 4)
Which of The following BEST represents the desired risk posture for an organization?

A. Inherent risk is lower than risk tolerance.
B. Operational risk is higher than risk tolerance.
C. Accepted risk is higher than risk tolerance.
D. Residual risk is lower than risk tolerance.

Answer: D

NEW QUESTION 17
- (Exam Topic 4)
Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?

A. Survey device owners.
B. Rescan the user environment.
C. Require annual end user policy acceptance.
D. Review awareness training assessment results

Answer: B

NEW QUESTION 19
- (Exam Topic 4)
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

A. To facilitate ongoing audit and control testing
B. To help manage risk to acceptable tolerance levels
C. To establish and maintain a control inventory
D. To increase the likelihood of effective control operation

Answer: D

NEW QUESTION 22
- (Exam Topic 4)
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

A. Collecting data for IT risk assessment
B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis

Answer: C

NEW QUESTION 26
- (Exam Topic 4)
A multinational organization is considering implementing standard background checks to' all new employees A KEY concern regarding this approach

A. fail to identity all relevant issues.
B. be too costly
C. violate laws in other countries
D. be too line consuming

Answer: C

NEW QUESTION 29
- (Exam Topic 4)
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

A. Review vendor control self-assessments (CSA).
B. Review vendor service level agreement (SLA) metrics.
C. Require independent control assessments.
D. Obtain vendor references from existing customers.

Answer: C

NEW QUESTION 33
- (Exam Topic 3)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

A. Identify changes in risk factors and initiate risk reviews.
B. Engage an external consultant to redesign the risk management process.
C. Outsource the process for updating the risk register.
D. Implement a process improvement and replace the old risk register.

Answer: A

NEW QUESTION 34
- (Exam Topic 4)
A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

A. Correct the vulnerabilities to mitigate potential risk exposure.
B. Develop a risk response action plan with key stakeholders.
C. Assess the level of risk associated with the vulnerabilities.
D. Communicate the vulnerabilities to the risk owner.

Answer: C

NEW QUESTION 35
- (Exam Topic 4)

Which of the following is MOST important to consider before determining a response to a vulnerability?

A. The likelihood and impact of threat events
B. The cost to implement the risk response
C. Lack of data to measure threat events
D. Monetary value of the asset

Answer: C

NEW QUESTION 37
- (Exam Topic 4)
Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

A. Risk control assessment
B. Audit reports with risk ratings
C. Penetration test results
D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 39
- (Exam Topic 3)
An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

A. Risk owner
B. IT security manager
C. IT system owner
D. Control owner

Answer: D

NEW QUESTION 44
- (Exam Topic 3)
Which of the following is the MOST effective control to maintain the integrity of system configuration files?

A. Recording changes to configuration files
B. Implementing automated vulnerability scanning
C. Restricting access to configuration documentation
D. Monitoring against the configuration standard

Answer: D

NEW QUESTION 45
- (Exam Topic 3)
Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

A. Evaluate the security architecture maturity.
B. Map the new requirements to the existing control framework.
C. Charter a privacy steering committee.
D. Conduct a privacy impact assessment (PIA).

Answer: D

NEW QUESTION 48
- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

A. Likelihood of a threat
B. Impact of technology risk
C. Impact of operational risk
D. Control weakness

Answer: C

NEW QUESTION 52
- (Exam Topic 3)
A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?

A. Periodic user privileges review
B. Log monitoring
C. Periodic internal audits
D. Segregation of duties

Answer: A

NEW QUESTION 57
- (Exam Topic 3)
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

A. Key risk indicators (KRIs)
B. Key management indicators (KMIs)
C. Key performance indicators (KPIs)
D. Key control indicators (KCIs)

Answer: D

NEW QUESTION 58
- (Exam Topic 3)
Which of the following is MOST helpful in preventing risk events from materializing?

A. Prioritizing and tracking issues
B. Establishing key risk indicators (KRIs)
C. Reviewing and analyzing security incidents
D. Maintaining the risk register

Answer: A

NEW QUESTION 60
- (Exam Topic 3)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

A. help an organization identify emerging threats.
B. benchmark the organization's risk profile.
C. identify trends in the organization's vulnerabilities.
D. enable ongoing monitoring of emerging risk.

Answer: D

NEW QUESTION 62
- (Exam Topic 3)
A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

A. Regulatory requirements may differ in each country.
B. Data sampling may be impacted by various industry restrictions.
C. Business advertising will need to be tailored by country.
D. The data analysis may be ineffective in achieving objectives.

Answer: A

NEW QUESTION 67
- (Exam Topic 3)
Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

A. Time required for backup restoration testing
B. Change in size of data backed up
C. Successful completion of backup operations
D. Percentage of failed restore tests

Answer: D

NEW QUESTION 69
- (Exam Topic 3)
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

A. Risk management strategy planning
B. Risk monitoring and control
C. Risk identification
D. Risk response planning

Answer: C

NEW QUESTION 74
- (Exam Topic 3)
The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

A. changes due to emergencies.
B. changes that cause incidents.
C. changes not requiring user acceptance testing.
D. personnel that have rights to make changes in production.

Answer:

B

NEW QUESTION 76
- (Exam Topic 3)
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

A. Conduct an abbreviated version of the assessment.
B. Report the business unit manager for a possible ethics violation.
C. Perform the assessment as it would normally be done.
D. Recommend an internal auditor perform the review.

Answer: B

NEW QUESTION 81
- (Exam Topic 3)
When of the following is the BEST key control indicator (KCI) to determine the effectiveness of en intrusion prevention system (IPS)?

A. Percentage of system uptime
B. Percentage of relevant threats mitigated
C. Total number of threats identified
D. Reaction time of the system to threats

Answer: B

NEW QUESTION 84
- (Exam Topic 3)
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

A. Risk manager
B. Data owner
C. End user
D. IT department

Answer: D

NEW QUESTION 88
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
B. Implement a key performance indicator (KPI) to monitor the existing control performance.
C. Accept the residual risk in its entirety and obtain executive management approval.
D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.

Answer: C

NEW QUESTION 93
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

A. Alignment with regulatory requirements
B. Availability of qualitative data
C. Properly set thresholds
D. Alignment with industry benchmarks

Answer: C

NEW QUESTION 95
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

A. mapping residual risk with cost of controls
B. comparing against regulatory requirements
C. comparing industry risk appetite with the organization's.
D. understanding the organization's risk appetite.

Answer: D

NEW QUESTION 97
- (Exam Topic 3)
When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

A. a identity conditions that may cause disruptions
B. Review incident response procedures
C. Evaluate the probability of risk events
D. Define metrics for restoring availability

Answer: A

NEW QUESTION 102
- (Exam Topic 3)
Which of the following should be determined FIRST when a new security vulnerability is made public?

A. Whether the affected technology is used within the organization
B. Whether the affected technology is Internet-facing
C. What mitigating controls are currently in place
D. How pervasive the vulnerability is within the organization

Answer: A

NEW QUESTION 104
- (Exam Topic 3)
When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

A. Users may share accounts with business system analyst
B. Application may not capture a complete audit trail.
C. Users may be able to circumvent application controls.
D. Multiple connects to the database are used and slow the process

Answer: C

NEW QUESTION 108
- (Exam Topic 3)
Which of the following should be of GREATEST concern lo a risk practitioner reviewing the implementation of an emerging technology?

A. Lack of alignment to best practices
B. Lack of risk assessment
C. Lack of risk and control procedures
D. Lack of management approval

Answer: B

NEW QUESTION 113
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

A. The sum of residual risk levels for each scenario
B. The loss expectancy for aggregated risk scenarios
C. The highest loss expectancy among the risk scenarios
D. The average of anticipated residual risk levels

Answer: D

NEW QUESTION 114
- (Exam Topic 3)
A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

A. Ensuring time synchronization of log sources.
B. Ensuring the inclusion of external threat intelligence log sources.
C. Ensuring the inclusion of all computing resources as log sources.
D. Ensuring read-write access to all log sources

Answer: A

NEW QUESTION 116
- (Exam Topic 3)
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

A. The number of users who can access sensitive data
B. A list of unencrypted databases which contain sensitive data
C. The reason some databases have not been encrypted
D. The cost required to enforce encryption

Answer: B

NEW QUESTION 118
- (Exam Topic 3)
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

A. Number of training sessions completed
B. Percentage of staff members who complete the training with a passing score
C. Percentage of attendees versus total staff
D. Percentage of staff members who attend the training with positive feedback

Answer: B

NEW QUESTION 123
- (Exam Topic 3)
Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?

A. Designing compensating controls
B. Determining if KRIs have been updated recently
C. Assessing the effectiveness of the incident response plan
D. Determining what has changed in the environment

Answer: D

NEW QUESTION 128
- (Exam Topic 3)
Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

A. Failed login attempts
B. Simulating a denial of service attack
C. Absence of IT audit findings
D. Penetration test

Answer: D

NEW QUESTION 131
- (Exam Topic 3)
During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

A. reset the alert threshold based on peak traffic
B. analyze the traffic to minimize the false negatives
C. analyze the alerts to minimize the false positives
D. sniff the traffic using a network analyzer

Answer: C

NEW QUESTION 135
- (Exam Topic 3)
Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information lo a supplier?

A. Encrypt the data while in transit lo the supplier
B. Contractually obligate the supplier to follow privacy laws.
C. Require independent audits of the supplier's control environment
D. Utilize blockchain during the data transfer

Answer: B

NEW QUESTION 140
- (Exam Topic 3)
A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

A. Escalate the concern to senior management.
B. Document the reasons for the exception.
C. Include the application in IT risk assessments.
D. Propose that the application be transferred to IT.

Answer: B

NEW QUESTION 143
- (Exam Topic 3)
Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

A. To create a complete repository of risk to the organization
B. To create a comprehensive view of critical risk to the organization
C. To provide a bottom-up view of the most significant risk scenarios
D. To optimize costs of managing risk scenarios in the organization

Answer: B

NEW QUESTION 145
- (Exam Topic 3)
Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

A. Percentage of legacy servers out of support
B. Percentage of severs receiving automata patches
C. Number of unremediated vulnerabilities
D. Number of intrusion attempts

Answer: D

NEW QUESTION 150
- (Exam Topic 3)
A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

A. include detailed deviations from industry benchmarks,
B. include a summary linking information to stakeholder needs,
C. include a roadmap to achieve operational excellence,
D. publish the report on-demand for stakeholders.

Answer: B

NEW QUESTION 155
- (Exam Topic 3)
An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager
B. Sales manager
C. Customer service manager
D. Access control manager

Answer: D

NEW QUESTION 158
- (Exam Topic 3)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

A. Ensuring that database changes are correctly applied
B. Enforcing that changes are authorized
C. Deterring illicit actions of database administrators
D. Preventing system developers from accessing production data

Answer: C

NEW QUESTION 161
- (Exam Topic 3)
Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

A. Building an organizational risk profile after updating the risk register
B. Ensuring risk owners participate in a periodic control testing process
C. Designing a process for risk owners to periodically review identified risk
D. Implementing a process for ongoing monitoring of control effectiveness

Answer: D

NEW QUESTION 164
- (Exam Topic 3)
Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

A. Establishing a disaster recovery plan (DRP)
B. Establishing recovery time objectives (RTOs)
C. Maintaining a current list of staff contact delays
D. Maintaining a risk register

Answer: D

NEW QUESTION 169
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

A. Personal data attributed to a specific data subject is tokenized.
B. Data protection impact assessments are performed on a regular basis.

C. Personal data certifications are performed to prevent excessive data collection.
D. Data retention guidelines are documented, established, and enforced.

Answer: B

NEW QUESTION 173
- (Exam Topic 3)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

A. Ability of the action plans to address multiple risk scenarios
B. Ease of implementing the risk treatment solution
C. Changes in residual risk after implementing the plans
D. Prioritization for implementing the action plans

Answer: C

NEW QUESTION 177
- (Exam Topic 3)
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

A. Third-party software is used for data analytics.
B. Data usage exceeds individual consent.
C. Revenue generated is not disclosed to customers.
D. Use of a data analytics system is not disclosed to customers.

Answer: B

NEW QUESTION 182
- (Exam Topic 3)
An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

A. The third party's IT operations manager
B. The organization's process owner
C. The third party's chief risk officer (CRO)
D. The organization's risk practitioner

Answer: B

NEW QUESTION 187
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

A. Least privilege access
B. Inability to edit
C. Ability to overwrite
D. Encryption

Answer: B

NEW QUESTION 191
- (Exam Topic 3)
To reduce costs, an organization is combining the second and third tines of defense in a new department that reports to a recently appointed C-level executive. Which of the following is the GREATEST concern with this situation?

A. The risk governance approach of the second and third lines of defense may differ.
B. The independence of the internal third line of defense may be compromised.
C. Cost reductions may negatively impact the productivity of other departments.
D. The new structure is not aligned to the organization's internal control framework.

Answer: B

NEW QUESTION 196
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

A. Analyze data protection methods.
B. Understand data flows.
C. Include a right-to-audit clause.
D. Implement strong access controls.

Answer: B

NEW QUESTION 198

- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

A. Enable data wipe capabilities
B. Penetration testing and session timeouts
C. Implement remote monitoring
D. Enforce strong passwords and data encryption

Answer: D

NEW QUESTION 203
- (Exam Topic 3)
What are the MOST essential attributes of an effective Key control indicator (KCI)?

A. Flexibility and adaptability
B. Measurability and consistency
C. Robustness and resilience
D. Optimal cost and benefit

Answer: B

NEW QUESTION 208
- (Exam Topic 3)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

A. Including trend analysis of risk metrics
B. Using an aggregated view of organizational risk
C. Relying on key risk indicator (KRI) data
D. Ensuring relevance to organizational goals

Answer: D

NEW QUESTION 210
- (Exam Topic 3)
The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs
B. can balance the overall technical and business concerns
C. can see the overall impact to the business
D. are more objective than information security management.

Answer: B

NEW QUESTION 214
- (Exam Topic 3)
Which of the following is the MOST important component in a risk treatment plan?

A. Technical details
B. Target completion date
C. Treatment plan ownership
D. Treatment plan justification

Answer: D

NEW QUESTION 219
- (Exam Topic 3)
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

A. Poor access control
B. Unnecessary data storage usage
C. Data inconsistency
D. Unnecessary costs of program changes

Answer: C

NEW QUESTION 224
- (Exam Topic 3)
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

A. Sufficient resources are not assigned to IT development projects.
B. Customer support help desk staff does not have adequate training.
C. Email infrastructure does not have proper rollback plans.
D. The corporate email system does not identify and store phishing emails.

Answer: A

NEW QUESTION 226
- (Exam Topic 3)
Which of the following is MOST important to the successful development of IT risk scenarios?

A. Cost-benefit analysis
B. Internal and external audit reports
C. Threat and vulnerability analysis
D. Control effectiveness assessment

Answer: C

NEW QUESTION 230
- (Exam Topic 3)
Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?

A. Adopting qualitative enterprise risk assessment methods
B. Linking IT risk scenarios to technology objectives
C. linking IT risk scenarios to enterprise strategy
D. Adopting quantitative enterprise risk assessment methods

Answer: C

NEW QUESTION 235
- (Exam Topic 3)
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

A. Conducting a business impact analysis (BIA)
B. Identifying the recovery response team
C. Procuring a recovery site
D. Assigning sensitivity levels to data

Answer: A

NEW QUESTION 238
- (Exam Topic 3)
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

A. Sharing company information on social media
B. Sharing personal information on social media
C. Using social media to maintain contact with business associates
D. Using social media for personal purposes during working hours

Answer: A

NEW QUESTION 241
- (Exam Topic 3)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

A. stakeholder risk tolerance.
B. benchmarking criteria.
C. suppliers used by the organization.
D. the control environment.

Answer: D

NEW QUESTION 242
- (Exam Topic 3)
Which of the following approaches BEST identifies information systems control deficiencies?

A. Countermeasures analysis
B. Best practice assessment
C. Gap analysis
D. Risk assessment

Answer: C

NEW QUESTION 246
- (Exam Topic 3)
Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

A. Data duplication processes
B. Data archival processes
C. Data anonymization processes
D. Data protection processes

Answer:

B

NEW QUESTION 247
- (Exam Topic 3)
Which of the following is the GREATEST advantage of implementing a risk management program?

A. Enabling risk-aware decisions
B. Promoting a risk-aware culture
C. Improving security governance
D. Reducing residual risk

Answer: A

NEW QUESTION 248
- (Exam Topic 3)
A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

A. Single sign-on
B. Audit trail review
C. Multi-factor authentication
D. Data encryption at rest

Answer: B

NEW QUESTION 251
- (Exam Topic 3)
Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

A. Threat event
B. Inherent risk
C. Risk event
D. Security incident

Answer: B

NEW QUESTION 255
- (Exam Topic 3)
Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

A. Requiring a printer access code for each user
B. Using physical controls to access the printer room
C. Using video surveillance in the printer room
D. Ensuring printer parameters are properly configured

Answer: A

NEW QUESTION 259
- (Exam Topic 3)
Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

A. Perform a gap analysis.
B. Prioritize impact to the business units.
C. Perform a risk assessment.
D. Review the risk tolerance and appetite.

Answer: C

NEW QUESTION 263
- (Exam Topic 3)
In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

A. A standardized risk taxonomy
B. A list of control deficiencies
C. An enterprise risk ownership policy
D. An updated risk tolerance metric

Answer: A

NEW QUESTION 264
- (Exam Topic 3)
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

A. Percentage of unpatched IT assets

B. Percentage of IT assets without ownership
C. The number of IT assets securely disposed during the past year
D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 266
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

A. select a provider to standardize the disaster recovery plans.
B. outsource disaster recovery to an external provider.
C. centralize the risk response function at the enterprise level.
D. evaluate opportunities to combine disaster recovery plans.

Answer: D

NEW QUESTION 269
- (Exam Topic 3)
An organization is implementing internet of Things (loT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

A. Insufficient network isolation
B. impact on network performance
C. insecure data transmission protocols
D. Lack of interoperability between sensors

Answer: D

NEW QUESTION 274
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

A. Risk ownership is recorded.
B. Vulnerabilities have separate entries.
C. Control ownership is recorded.
D. Residual risk is less than inherent risk.

Answer: A

NEW QUESTION 276
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

A. Prioritize risk response options
B. Reduce likelihood.
C. Address more than one risk response
D. Reduce impact

Answer: C

NEW QUESTION 277
- (Exam Topic 4)
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

A. Reviewing the results of independent audits
B. Performing a site visit to the cloud provider's data center
C. Performing a due diligence review
D. Conducting a risk workshop with key stakeholders

Answer: D

NEW QUESTION 280
- (Exam Topic 4)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help lo prevent technical vulnerabilities from being exploded?

A. implement code reviews and Quality assurance on a regular basis
B. Verity me software agreement indemnifies the company from losses
C. Review the source coda and error reporting of the application
D. Update the software with the latest patches and updates

Answer: D

NEW QUESTION 284
- (Exam Topic 4)
A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?

A. Enable data encryption in the test environment.
B. Prevent the use of production data in the test environment
C. De-identify data before being transferred to the test environment.
D. Enforce multi-factor authentication within the test environment.

Answer: C

NEW QUESTION 288
- (Exam Topic 4)
Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

A. Organizational structure and job descriptions
B. Risk appetite and risk tolerance
C. Industry best practices for risk management
D. Prior year's risk assessment results

Answer: B

NEW QUESTION 291
- (Exam Topic 4)
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

A. Management may be unable to accurately evaluate the risk profile.
B. Resources may be inefficiently allocated.
C. The same risk factor may be identified in multiple areas.
D. Multiple risk treatment efforts may be initiated to treat a given risk.

Answer: A

NEW QUESTION 295
- (Exam Topic 4)
Who should be responsible (of evaluating the residual risk after a compensating control has been

A. Compliance manager
B. Risk owner
C. Control owner
D. Risk practitioner

Answer: D

NEW QUESTION 298
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

A. KRIs assist in the preparation of the organization's risk profile.
B. KRIs signal that a change in the control environment has occurred.
C. KRIs provide a basis to set the risk appetite for an organization
D. KRIs provide an early warning that a risk threshold is about to be reached.

Answer: D

NEW QUESTION 302
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

A. Assigning a data owner
B. Implementing technical control over the assets
C. Implementing a data loss prevention (DLP) solution
D. Scheduling periodic audits

Answer: A

NEW QUESTION 307
- (Exam Topic 4)
Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

A. Results of a business impact analysis (BIA)
B. Risk assessment results
C. A mapping of resources to business processes
D. Key performance indicators (KPIs)

Answer:

B

NEW QUESTION 311
- (Exam Topic 4)
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

A. Remove risk that has been mitigated by third-party transfer
B. Remove risk that management has decided to accept
C. Remove risk only following a significant change in the risk environment
D. Remove risk when mitigation results in residual risk within tolerance levels

Answer: C

NEW QUESTION 314
- (Exam Topic 4)
Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

A. Perform a gap analysis
B. Conduct system testing
C. Implement compensating controls
D. Update security policies

Answer: A

NEW QUESTION 317
- (Exam Topic 4)
When performing a risk assessment of a new service to support a core business process, which of the following should be done FIRST to ensure continuity of operations?

A. Define metrics for restoring availability.
B. Identify conditions that may cause disruptions.
C. Review incident response procedures.
D. Evaluate the probability of risk events.

Answer: B

NEW QUESTION 320
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

A. Verifying that project objectives are met
B. Identifying project cost overruns
C. Leveraging an independent review team
D. Reviewing the project initiation risk matrix

Answer: A

NEW QUESTION 325
- (Exam Topic 4)
An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

A. Employees
B. Data
C. Reputation
D. Customer lists

Answer: A

NEW QUESTION 330
- (Exam Topic 4)
The MAIN reason for prioritizing IT risk responses is to enable an organization to:

A. determine the risk appetite.
B. determine the budget.
C. define key performance indicators (KPIs).
D. optimize resource utilization.

Answer: C

NEW QUESTION 332
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

A. Key risk indicators (KRIs)
B. Documented procedures

C. Information security policies
D. Information security standards

Answer: B

NEW QUESTION 335
- (Exam Topic 4)
Which of the following is the MOST important reason to validate that risk responses have been executed as outlined in the risk response plan''

A. To ensure completion of the risk assessment cycle
B. To ensure controls arc operating effectively
C. To ensure residual risk Is at an acceptable level
D. To ensure control costs do not exceed benefits

Answer: A

NEW QUESTION 337
- (Exam Topic 4)
When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

A. risk exposure in business terms
B. a detailed view of individual risk exposures
C. a summary of incidents that have impacted the organization.
D. recommendations by an independent risk assessor.

Answer: A

NEW QUESTION 342
- (Exam Topic 4)
Which of the following is the PRIMARY objective of risk management?

A. Identify and analyze risk.
B. Achieve business objectives
C. Minimi2e business disruptions.
D. Identify threats and vulnerabilities.

Answer: B

NEW QUESTION 345
- (Exam Topic 4)
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner s NEXT step? r

A. Prepare a business case for the response options.
B. Identify resources for implementing responses.
C. Develop a mechanism for monitoring residual risk.
D. Update the risk register with the results.

Answer: D

NEW QUESTION 346
- (Exam Topic 4)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

A. The volume of risk scenarios is too large
B. Risk aggregation has not been completed
C. Risk scenarios are not applicable
D. The risk analysts for each scenario is incomplete

Answer: D

NEW QUESTION 350
- (Exam Topic 4)
Who is MOST important lo include in the assessment of existing IT risk scenarios?

A. Technology subject matter experts
B. Business process owners
C. Business users of IT systems
D. Risk management consultants

Answer: C

NEW QUESTION 352
- (Exam Topic 4)

The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

A. data logging and monitoring
B. data mining and analytics
C. data classification and labeling
D. data retention and destruction

Answer: C

NEW QUESTION 356
- (Exam Topic 4)
One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

A. Additional mitigating controls should be identified.
B. The system should not be used until the application is changed
C. The organization's IT risk appetite should be adjusted.
D. The associated IT risk should be accepted by management.

Answer: A

NEW QUESTION 358
- (Exam Topic 4)
Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

A. Control owner
B. Risk owner
C. Internal auditor
D. Compliance manager

Answer: C

NEW QUESTION 362
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

A. Risk avoidance
B. Risk transfer
C. Risk mitigation
D. Risk acceptance

Answer: A

NEW QUESTION 363
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

A. Service level agreements (SLAs) have not been met over the last quarter.
B. The service contract is up for renewal in less than thirty days.
C. Key third-party personnel have recently been replaced.
D. Monthly service charges are significantly higher than industry norms.

Answer: C

NEW QUESTION 368
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap
B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 371
- (Exam Topic 4)
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

A. Increase in mitigating control costs
B. Increase in risk event impact
C. Increase in risk event likelihood
D. Increase in cybersecurity premium

Answer: C

NEW QUESTION 374
- (Exam Topic 4)
When defining thresholds for control key performance indicators (KPIs). it is MOST helpful to align:

A. information risk assessments with enterprise risk assessments.
B. key risk indicators (KRIs) with risk appetite of the business.
C. the control key performance indicators (KPIs) with audit findings.
D. control performance with risk tolerance of business owners.

Answer: B

NEW QUESTION 376
- (Exam Topic 4)
Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database"

A. Implement role-based access control
B. Implement a data masking process
C. Include sanctions in nondisclosure agreements (NDAs)
D. Install a data loss prevention (DLP) tool

Answer: A

NEW QUESTION 377
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

A. Absorb the loss in productivity.
B. Request a waiver to the requirements.
C. Escalate the issue to senior management
D. Remove the control to accommodate business objectives.

Answer: C

NEW QUESTION 381
- (Exam Topic 4)
Which of the following should be considered FIRST when creating a comprehensive IT risk register?

A. Risk management budget
B. Risk mitigation policies
C. Risk appetite
D. Risk analysis techniques

Answer: C

NEW QUESTION 386
- (Exam Topic 4)
An organization has experienced a cyber attack that exposed customer personally identifiable information (Pll) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact
D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 390
- (Exam Topic 4)
Which of the following is the GREATEST benefit of centralizing IT systems?

A. Risk reporting
B. Risk classification
C. Risk monitoring
D. Risk identification

Answer: C

NEW QUESTION 391
- (Exam Topic 4)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

A. Acquisition
B. Implementation
C. Initiation

D. Operation and maintenance

Answer: C

NEW QUESTION 395
- (Exam Topic 4)
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

A. The report was provided directly from the vendor.
B. The risk associated with multiple control gaps was accepted.
C. The control owners disagreed with the auditor's recommendations.
D. The controls had recurring noncompliance.

Answer: A

NEW QUESTION 397
- (Exam Topic 4)
Which of the following is MOST important for successful incident response?

A. The quantity of data logged by the attack control tools
B. Blocking the attack route immediately
C. The ability to trace the source of the attack
D. The timeliness of attack recognition

Answer: D

NEW QUESTION 398
- (Exam Topic 4)
Which of the following is MOST important to promoting a risk-aware culture?

A. Regular testing of risk controls
B. Communication of audit findings
C. Procedures for security monitoring
D. Open communication of risk reporting

Answer: D

NEW QUESTION 402
- (Exam Topic 4)
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the risk practitioner do NEXT?

A. Identify new threats resorting from the new business strategy
B. Update risk awareness training to reflect current levels of risk appetite and tolerance
C. Inform the board of potential risk scenarios associated with aggressive business strategies
D. Increase the scale for measuring impact due to threat materialization

Answer: A

NEW QUESTION 404
- (Exam Topic 4)
The MAJOR reason to classify information assets is

A. maintain a current inventory and catalog of information assets
B. determine their sensitivity and critical
C. establish recovery time objectives (RTOs)
D. categorize data into groups

Answer: C

NEW QUESTION 407
- (Exam Topic 4)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

A. Risk management treatment plan
B. Risk assessment results
C. Risk management framework
D. Risk register

Answer: C

NEW QUESTION 408
- (Exam Topic 4)
Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

A. To provide input to the organization's risk appetite
B. To monitor the vendor's control effectiveness
C. To verify the vendor's ongoing financial viability
D. To assess the vendor's risk mitigation plans

Answer: B

NEW QUESTION 412
- (Exam Topic 4)
In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

A. system architecture in target areas.
B. IT management policies and procedures.
C. business objectives of the organization.
D. defined roles and responsibilities.

Answer: D

NEW QUESTION 414
- (Exam Topic 4)
The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

A. Insufficient risk tolerance
B. Optimized control management
C. Effective risk management
D. Over-controlled environment

Answer: B

NEW QUESTION 418
- (Exam Topic 4)
Which of the following is the BEST approach for selecting controls to minimize risk?

A. Industry best practice review
B. Risk assessment
C. Cost-benefit analysis
D. Control-effectiveness evaluation

Answer: C

NEW QUESTION 422
- (Exam Topic 4)
When creating a separate IT risk register for a large organization, which of the following is MOST important to consider with regard to the existing corporate risk 'register?

A. Leveraging business risk professionals
B. Relying on generic IT risk scenarios
C. Describing IT risk in business terms
D. Using a common risk taxonomy

Answer: D

NEW QUESTION 427
- (Exam Topic 4)
Which of the following is the BEST method of creating risk awareness in an organization?

A. Marking the risk register available to project stakeholders
B. Ensuring senior management commitment to risk training
C. Providing regular communication to risk managers
D. Appointing the risk manager from the business units

Answer: B

NEW QUESTION 431
- (Exam Topic 4)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

A. Ability to determine business impact
B. Up-to-date knowledge on risk responses
C. Decision-making authority for risk treatment
D. Awareness of emerging business threats

Answer: A

NEW QUESTION 436

- (Exam Topic 4)
Which of the following provides the MOST reliable evidence of a control's effectiveness?

A. A risk and control self-assessment
B. Senior management's attestation
C. A system-generated testing report
D. detailed process walk-through

Answer: D

NEW QUESTION 438
- (Exam Topic 4)
Effective risk communication BEST benefits an organization by:

A. helping personnel make better-informed decisions
B. assisting the development of a risk register.
C. improving the effectiveness of IT controls.
D. increasing participation in the risk assessment process.

Answer: A

NEW QUESTION 442
- (Exam Topic 4)
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

A. Limited organizational knowledge of the underlying technology
B. Lack of commercial software support
C. Varying costs related to implementation and maintenance
D. Slow adoption of the technology across the financial industry

Answer: A

NEW QUESTION 443
- (Exam Topic 4)
Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

A. Changes in the organization's risk appetite and risk tolerance levels
B. Impact due to changes in external and internal risk factors
C. Changes in residual risk levels against acceptable levels
D. Gaps in best practices and implemented controls across the industry

Answer: C

NEW QUESTION 447
- (Exam Topic 4)
A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

A. mature
B. ineffective.
C. optimized.
D. inefficient.

Answer: B

NEW QUESTION 452
- (Exam Topic 4)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

A. Number of service level agreement (SLA) violations
B. Percentage of recovery issues identified during the exercise
C. Number of total systems recovered within tie recovery point objective (RPO)
D. Percentage of critical systems recovered within tie recovery time objective (RTO)

Answer: D

NEW QUESTION 456
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which ot the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.

Answer: A

NEW QUESTION 461
- (Exam Topic 4)
Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

A. Compliance manager
B. Data architect
C. Data owner
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 464
- (Exam Topic 4)
Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

A. Risk owner
B. Risk practitioner
C. Compliance manager
D. Control owner

Answer: B

NEW QUESTION 469
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

A. testing requirements
B. the implementation plan.
C. System requirements
D. The security policy

Answer: C

NEW QUESTION 471
- (Exam Topic 4)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

A. Accountability is established for risk treatment decisions
B. Stakeholders are consulted about risk treatment options
C. Risk owners are informed of risk treatment options
D. Responsibility is established for risk treatment decisions.

Answer: A

NEW QUESTION 473
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

A. To identify gaps in data protection controls
B. To develop a customer notification plan
C. To identify personally identifiable information (Pll)
D. To determine gaps in data identification processes

Answer: A

NEW QUESTION 478
- (Exam Topic 4)
An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

A. Reassess whether mitigating controls address the known risk in the processes.
B. Update processes to address the new technology.
C. Update the data governance policy to address the new technology.
D. Perform a gap analysis of the impacted processes.

Answer: A

NEW QUESTION 483
- (Exam Topic 4)
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

A. Analyzing cyber intelligence reports
B. Engaging independent cybersecurity consultants
C. Increasing the frequency of updates to the risk register
D. Reviewing the outcome of the latest security risk assessment

Answer: D

NEW QUESTION 484
- (Exam Topic 4)
A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

A. Risk manager
B. Control owner
C. Control tester
D. Risk owner

Answer: B

NEW QUESTION 489
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

A. Regulatory requirements
B. Organizational objectives
C. Annual loss expectancy (ALE)
D. Risk management costs

Answer: C

NEW QUESTION 493
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

A. Risk likelihood
B. Risk culture
C. Risk appetite
D. Risk capacity

Answer: A

NEW QUESTION 496
- (Exam Topic 4)
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

A. prepare a follow-up risk assessment.
B. recommend acceptance of the risk scenarios.
C. reconfirm risk tolerance levels.
D. analyze changes to aggregate risk.

Answer: D

NEW QUESTION 500
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

Answer: A

NEW QUESTION 501
- (Exam Topic 3)
Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

A. The risk profile was not updated after a recent incident
B. The risk profile was developed without using industry standards.
C. The risk profile was last reviewed two years ago.
D. The risk profile does not contain historical loss data.

Answer: A

NEW QUESTION 503

- (Exam Topic 3)
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

A. Activity logging and monitoring
B. Periodic access review
C. Two-factor authentication
D. Awareness training and background checks

Answer: A

NEW QUESTION 506
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual
risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

A. Identify new risk entries to include in ERM.
B. Remove the risk entries from the ERM register.
C. Re-perform the risk assessment to confirm results.
D. Verify the adequacy of risk monitoring plans.

Answer: D

NEW QUESTION 510
- (Exam Topic 3)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

A. External audit
B. Internal audit
C. Vendor performance scorecard
D. Regulatory examination

Answer: A

NEW QUESTION 513
- (Exam Topic 3)
Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?

A. KCIs are independent from KRIs KRIs.
B. KCIs and KRIs help in determining risk appetite.
C. KCIs are defined using data from KRIs.
D. KCIs provide input for KRIs

Answer: D

NEW QUESTION 518
- (Exam Topic 3)
A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

A. Align applications to business processes.
B. Implement an enterprise architecture (EA).
C. Define the software development life cycle (SDLC).
D. Define enterprise-wide system procurement requirements.

Answer: B

NEW QUESTION 520
- (Exam Topic 3)
When an organization’s disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

A. Acceptance
B. Mitigation
C. Transfer
D. Avoidance

Answer: B

NEW QUESTION 524
- (Exam Topic 3)
Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

A. Regulatory compliance
B. Risk ownership
C. Best practices
D. Desired risk level

Answer: D

NEW QUESTION 528
- (Exam Topic 3)
Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

A. User authorization
B. User recertification
C. Change log review
D. Access log monitoring

Answer: B

NEW QUESTION 529
- (Exam Topic 3)
Which of the following BEST indicates that additional or improved controls ate needed m the environment?

A. Management, has decreased organisational risk appetite
B. The risk register and portfolio do not include all risk scenarios
C. merging risk scenarios have been identified
D. Risk events and losses exceed risk tolerance

Answer: D

NEW QUESTION 533
- (Exam Topic 3)
Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

A. A comparison of the costs of notice and consent control options
B. Examples of regulatory fines incurred by industry peers for noncompliance
C. A report of critical controls showing the importance of notice and consent
D. A cost-benefit analysis of the control versus probable legal action

Answer: D

NEW QUESTION 534
- (Exam Topic 3)
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

A. Transfer
B. Mitigation
C. Avoidance
D. Acceptance

Answer: D

NEW QUESTION 536
- (Exam Topic 3)
Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

A. Privacy risk controls
B. Business continuity
C. Risk taxonomy
D. Management support

Answer: A

NEW QUESTION 541
- (Exam Topic 3)
Which of the following BEST assists in justifying an investment in automated controls?

A. Cost-benefit analysis
B. Alignment of investment with risk appetite

C. Elimination of compensating controls
D. Reduction in personnel costs

Answer: A

NEW QUESTION 545
- (Exam Topic 3)
An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

A. The balanced scorecard
B. A cost-benefit analysis
C. The risk management frameworkD, A roadmap of IT strategic planning

Answer: B

NEW QUESTION 548
- (Exam Topic 3)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

A. Ensure compliance.
B. Identify trends.
C. Promote a risk-aware culture.
D. Optimize resources needed for controls

Answer: A

NEW QUESTION 552
- (Exam Topic 3)
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

A. resources to monitor backups
B. restoration monitoring reports
C. backup recovery requests
D. recurring restore failures

Answer: D

NEW QUESTION 556
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

A. Decreased success rate of internal phishing tests
B. Decreased number of reported security incidents
C. Number of disciplinary actions issued for security violations
D. Number of employees that complete security training

Answer: A

NEW QUESTION 558
- (Exam Topic 3)
An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

A. Conduct a risk analysis.
B. Initiate a remote data wipe.
C. Invoke the incident response plan
D. Disable the user account.

Answer: C

NEW QUESTION 559
- (Exam Topic 3)
An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

A. a lack of mitigating actions for identified risk
B. decreased threat levels
C. ineffective service delivery
D. ineffective IT governance

Answer: D

NEW QUESTION 562
- (Exam Topic 3)
Which of the following is the BEST way to assess the effectiveness of an access management process?

A. Comparing the actual process with the documented process
B. Reviewing access logs for user activity
C. Reconciling a list of accounts belonging to terminated employees
D. Reviewing for compliance with acceptable use policy

Answer: B

NEW QUESTION 567
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

A. Percentage of job failures identified and resolved during the recovery process
B. Percentage of processes recovered within the recovery time and point objectives
C. Number of current test plans and procedures
D. Number of issues and action items resolved during the recovery test

Answer: B

NEW QUESTION 570
- (Exam Topic 3)
Which of the following will BEST help in communicating strategic risk priorities?

A. Heat map
B. Business impact analysis (BIA)
C. Balanced Scorecard
D. Risk register

Answer: A

NEW QUESTION 575
- (Exam Topic 3)
Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

A. To provide data for establishing the risk profile
B. To provide assurance of adherence to risk management policies
C. To provide measurements on the potential for risk to occur
D. To provide assessments of mitigation effectiveness

Answer: D

NEW QUESTION 576
- (Exam Topic 3)
A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

A. management.
B. tolerance.
C. culture.
D. analysis.

Answer: C

NEW QUESTION 577
- (Exam Topic 3)
Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

A. Key audit findings
B. Treatment plan status
C. Performance indicators
D. Risk scenario results

Answer: C

NEW QUESTION 579
- (Exam Topic 3)
Which of the following should be done FIRST when information is no longer required to support business objectives?

A. Archive the information to a backup database.
B. Protect the information according to the classification policy.
C. Assess the information against the retention policy.
D. Securely and permanently erase the information

Answer: C

NEW QUESTION 580

- (Exam Topic 3)
In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

A. Educating employees on what needs to be kept confidential
B. Implementing a data loss prevention (DLP) solution
C. Taking punitive action against employees who expose confidential data
D. Requiring employees to sign nondisclosure agreements

Answer: B

NEW QUESTION 582
- (Exam Topic 3)
In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

A. two-factor authentication.
B. continuous data backup controls.
C. encryption for data at rest.
D. encryption for data in motion.

Answer: B

NEW QUESTION 584
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

A. Unknown vulnerabilities
B. Legacy technology systems
C. Network isolation
D. Overlapping threats

Answer: D

NEW QUESTION 586
- (Exam Topic 3)
Which of me following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

A. Identifying tweets that may compromise enterprise architecture (EA)
B. Including diverse Business scenarios in user acceptance testing (UAT)
C. Performing risk assessments during the business case development stage
D. Including key stakeholders in review of user requirements

Answer: D

NEW QUESTION 590
- (Exam Topic 3)
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

A. Conduct a comprehensive review of access management processes.
B. Declare a security incident and engage the incident response team.
C. Conduct a comprehensive awareness session for system administrators.
D. Evaluate system administrators' technical skills to identify if training is required.

Answer: A

NEW QUESTION 591
- (Exam Topic 3)
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

A. Complete an offsite business continuity exercise.
B. Conduct a compliance check against standards.
C. Perform a vulnerability assessment.
D. Measure the change in inherent risk.

Answer: C

NEW QUESTION 594
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

A. Detective
B. Directive
C. Preventive
D. Compensating

Answer: B

NEW QUESTION 599
- (Exam Topic 3)
For a large software development project, risk assessments are MOST effective when performed:

A. before system development begins.
B. at system development.
C. at each stage of the system development life cycle (SDLC).
D. during the development of the business case.

Answer: C

NEW QUESTION 603
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

A. Manage cyber risk according to the organization's risk management framework.
B. Define cyber roles and responsibilities across the organization
C. Conduct cyber risk awareness training tailored specifically for senior management
D. Implement a cyber risk program based on industry best practices

Answer: B

NEW QUESTION 607
- (Exam Topic 3)
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

A. Control self-assessment (CSA)
B. Security information and event management (SIEM) solutions
C. Data privacy impact assessment (DPIA)
D. Data loss prevention (DLP) tools

Answer: B

NEW QUESTION 610
- (Exam Topic 3)
Which of the following presents the GREATEST risk to change control in business application development over the complete life cycle?

A. Emphasis on multiple application testing cycles
B. Lack of an integrated development environment (IDE) tool
C. Introduction of requirements that have not been approved
D. Bypassing quality requirements before go-live

Answer: C

NEW QUESTION 611
- (Exam Topic 3)
Which of the following is the MOST effective way to integrate risk and compliance management?

A. Embedding risk management into compliance decision-making
B. Designing corrective actions to improve risk response capabilities
C. Embedding risk management into processes that are aligned with business drivers
D. Conducting regular self-assessments to verify compliance

Answer: A

NEW QUESTION 613
- (Exam Topic 3)
Which of the following would BEST help to address the risk associated with malicious outsiders modifying application data?

A. Multi-factor authentication
B. Role-based access controls
C. Activation of control audits
D. Acceptable use policies

Answer: A

NEW QUESTION 614
- (Exam Topic 3)
Accountability for a particular risk is BEST represented in a:

A. risk register
B. risk catalog
C. risk scenario

D. RACI matrix

Answer: D

NEW QUESTION 616
- (Exam Topic 3)
An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

A. Balanced scorecard
B. Capability maturity level
C. Internal audit plan
D. Control self-assessment (CSA)

Answer: A

NEW QUESTION 621
- (Exam Topic 3)
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

A. AI requires entirely new risk management processes.
B. AI potentially introduces new types of risk.
C. AI will result in changes to business processes.
D. Third-party AI solutions increase regulatory obligations.

Answer: B

NEW QUESTION 623
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

A. Implement database activity and capacity monitoring.
B. Ensure the business is aware of the risk.
C. Ensure the enterprise has a process to detect such situations.
D. Consider providing additional system resources to this job.

Answer: C

NEW QUESTION 625
- (Exam Topic 2)
An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

A. Feedback from end users
B. Results of a benchmark analysis
C. Recommendations from internal audit
D. Prioritization from business owners

Answer: D

NEW QUESTION 630
- (Exam Topic 2)
Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

A. Loss expectancy information
B. Control performance predictions
C. IT service level agreements (SLAs)
D. Remediation activity progress

Answer: A

NEW QUESTION 633
- (Exam Topic 2)
Mapping open risk issues to an enterprise risk heat map BEST facilitates:

A. risk response.
B. control monitoring.
C. risk identification.
D. risk ownership.

Answer: A

NEW QUESTION 638

- (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?

A. Quantified risk triggers
B. Cost of controls
C. Regulatory requirements
D. Organizational goals

Answer: D

NEW QUESTION 640
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

A. Identifying monitoring mechanisms
B. Including them in the risk register
C. Aligning them with business objectives
D. Prototyping compensating controls

Answer: C

NEW QUESTION 641
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

A. Include the new risk scenario in the current risk assessment.
B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 643
- (Exam Topic 2)
Which of the following is a detective control?

A. Limit check
B. Periodic access review
C. Access control software
D. Rerun procedures

Answer: B

NEW QUESTION 645
- (Exam Topic 2)
Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

A. Audit and compliance management
B. The chief information officer (CIO) and the chief financial officer (CFO)
C. Enterprise risk management and business process owners
D. Executive management and the board of directors

Answer: D

NEW QUESTION 650
- (Exam Topic 2)
The BEST way to test the operational effectiveness of a data backup procedure is to:

A. conduct an audit of files stored offsite.
B. interview employees to compare actual with expected procedures.
C. inspect a selection of audit trails and backup logs.
D. demonstrate a successful recovery from backup files.

Answer: D

NEW QUESTION 654
- (Exam Topic 2)
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

A. An antivirus program
B. Database activity monitoring
C. Firewall log monitoring
D. File integrity monitoring

Answer: C

NEW QUESTION 658
- (Exam Topic 2)
An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

A. A recommendation for internal audit validation
B. Plans for mitigating the associated risk
C. Suggestions for improving risk awareness training
D. The impact to the organization's risk profile

Answer: D

NEW QUESTION 659
- (Exam Topic 2)
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

A. Enhance the security awareness program.
B. Increase the frequency of incident reporting.
C. Purchase cyber insurance from a third party.
D. Conduct a control assessment.

Answer: D

NEW QUESTION 661
- (Exam Topic 2)
The PRIMARY purpose of a maturity model is to compare the:

A. current state of key processes to their desired state.
B. actual KPIs with target KPIs.
C. organization to industry best practices.
D. organization to peers.

Answer: A

NEW QUESTION 662
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the use of data analytics?

A. Distributed data sources
B. Manual data extraction
C. Incorrect data selection
D. Excessive data volume

Answer: C

NEW QUESTION 666
- (Exam Topic 2)
Which of the following is MOST essential for an effective change control environment?

A. Business management approval of change requests
B. Separation of development and production environments
C. Requirement of an implementation rollback plan
D. IT management review of implemented changes

Answer: A

NEW QUESTION 667
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

A. Key risk indicators (KRIs)
B. Data backups
C. Incident response plan
D. Cyber insurance

Answer: C

NEW QUESTION 671
- (Exam Topic 2)
An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

A. External resources may need to be involved.
B. Data privacy regulations may be violated.
C. Recovery costs may increase significantly.
D. Service interruptions may be longer than anticipated.

Answer:

D

NEW QUESTION 672
- (Exam Topic 2)
Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

A. Nondisclosure agreement (NDA)
B. Independent audit report
C. Business impact analysis (BIA)
D. Service level agreement (SLA)

Answer: B

NEW QUESTION 677
- (Exam Topic 2)
Which of the following is the BEST approach for determining whether a risk action plan is effective?

A. Comparing the remediation cost against budget
B. Assessing changes in residual risk
C. Assessing the inherent risk
D. Monitoring changes of key performance indicators (KPIs)

Answer: B

NEW QUESTION 679
- (Exam Topic 2)
Which of the following is MOST influential when management makes risk response decisions?

A. Risk appetite
B. Audit risk
C. Residual risk
D. Detection risk

Answer: A

NEW QUESTION 684
- (Exam Topic 2)
Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

A. Engaging external risk professionals to periodically review the risk
B. Prioritizing global standards over local requirements in the risk profile
C. Updating the risk profile with risk assessment results
D. Assigning quantitative values to qualitative metrics in the risk register

Answer: C

NEW QUESTION 688
- (Exam Topic 2)
Which of the following will BEST help ensure that risk factors identified during an information systems review are addressed?

A. Informing business process owners of the risk
B. Reviewing and updating the risk register
C. Assigning action items and deadlines to specific individuals
D. Implementing new control technologies

Answer: C

NEW QUESTION 690
- (Exam Topic 2)
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

A. An internal audit
B. Security operations center review
C. Internal penetration testing
D. A third-party audit

Answer: D

NEW QUESTION 694
- (Exam Topic 2)
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

A. Recommend avoiding the risk.
B. Validate the risk response with internal audit.
C. Update the risk register.

D. Evaluate outsourcing the process.

Answer: C

NEW QUESTION 696
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

A. Risk policy review
B. Business impact analysis (B1A)
C. Control catalog
D. Risk register

Answer: D

NEW QUESTION 700
- (Exam Topic 2)
What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

A. Relative positions on the risk map
B. Risk treatment options
C. Capability of enterprise to implement
D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 704
- (Exam Topic 2)
As part of an overall IT risk management plan, an IT risk register BEST helps management:

A. align IT processes with business objectives.
B. communicate the enterprise risk management policy.
C. stay current with existing control status.
D. understand the organizational risk profile.

Answer: D

NEW QUESTION 707
- (Exam Topic 2)
Which of the following is MOST critical to the design of relevant risk scenarios?

A. The scenarios are based on past incidents.
B. The scenarios are linked to probable organizational situations.
C. The scenarios are mapped to incident management capabilities.
D. The scenarios are aligned with risk management capabilities.

Answer: B

NEW QUESTION 710
- (Exam Topic 2)
Which of the following will BEST help to ensure that information system controls are effective?

A. Responding promptly to control exceptions
B. Implementing compensating controls
C. Testing controls periodically
D. Automating manual controls

Answer: C

NEW QUESTION 714
- (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.
C. verify Internet firewall control settings.

D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 717
- (Exam Topic 2)
An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

A. rolled back changes below management's thresholds.
B. change-related exceptions per month.
C. the average implementation time for changes.
D. number of user stories approved for implementation.

Answer: B

NEW QUESTION 718
- (Exam Topic 2)
Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

A. Vulnerability scanning
B. Continuous monitoring and alerting
C. Configuration management
D. Access controls and active logging

Answer: C

NEW QUESTION 722
- (Exam Topic 2)
Which of the following should an organization perform to forecast the effects of a disaster?

A. Develop a business impact analysis (BIA).
B. Define recovery time objectives (RTO).
C. Analyze capability maturity model gaps.
D. Simulate a disaster recovery.

Answer: A

NEW QUESTION 727
- (Exam Topic 2)
Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

A. An acceptable use policy for personal devices
B. Required user log-on before synchronizing data
C. Enforced authentication and data encryption
D. Security awareness training and testing

Answer: C

NEW QUESTION 730
- (Exam Topic 2)
Reviewing which of the following provides the BEST indication of an organizations risk tolerance?

A. Risk sharing strategy
B. Risk transfer agreements
C. Risk policies
D. Risk assessments

Answer: D

NEW QUESTION 733
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

A. Annual loss expectancy (ALE)
B. Business impact analysis
C. Cost-benefit analysis
D. Inherent vulnerabilities

Answer: A

NEW QUESTION 738
- (Exam Topic 2)
Which of the following would prompt changes in key risk indicator {KRI) thresholds?

A. Changes to the risk register

B. Changes in risk appetite or tolerance
C. Modification to risk categories
D. Knowledge of new and emerging threats

Answer: B

NEW QUESTION 739
- (Exam Topic 2)
Within the three lines of defense model, the accountability for the system of internal control resides with:

A. the chief information officer (CIO).
B. the board of directors
C. enterprise risk management
D. the risk practitioner

Answer: B

NEW QUESTION 744
- (Exam Topic 2)
Which of the following BEST supports the communication of risk assessment results to stakeholders?

A. Monitoring of high-risk areas
B. Classification of risk profiles
C. Periodic review of the risk register
D. Assignment of risk ownership

Answer: D

NEW QUESTION 749
- (Exam Topic 2)
A risk practitioner has observed that risk owners have approved a high number of exceptions to the information security policy. Which of the following should be the risk practitioner's GREATEST concern?

A. Security policies are being reviewed infrequently.
B. Controls are not operating efficiently.
C. Vulnerabilities are not being mitigated
D. Aggregate risk is approaching the tolerance threshold

Answer: D

NEW QUESTION 753
- (Exam Topic 2)
Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

A. review the key risk indicators.
B. conduct a risk analysis.
C. update the risk register
D. reallocate risk response resources.

Answer: A

NEW QUESTION 756
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

A. Time between control failure and failure detection
B. Number of key controls as a percentage of total control count
C. Time spent on internal control assessment reviews
D. Number of internal control failures within the measurement period

Answer: A

NEW QUESTION 759
- (Exam Topic 2)
Which of the following is the MOST important input when developing risk scenarios?

A. Key performance indicators
B. Business objectives
C. The organization's risk framework
D. Risk appetite

Answer: B

NEW QUESTION 761

- (Exam Topic 2)
To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

A. During the business requirement definitions phase
B. Before periodic steering committee meetings
C. At each stage of the development life cycle
D. During the business case development

Answer: A

NEW QUESTION 763
- (Exam Topic 2)
Which of the following is the BEST way to determine software license compliance?

A. List non-compliant systems in the risk register.
B. Conduct periodic compliance reviews.
C. Review whistlebtower reports of noncompliance.
D. Monitor user software download activity.

Answer: B

NEW QUESTION 765
- (Exam Topic 2)
The maturity of an IT risk management program is MOST influenced by:

A. the organization's risk culture
B. benchmarking results against similar organizations
C. industry-specific regulatory requirements
D. expertise available within the IT department

Answer: A

NEW QUESTION 766
- (Exam Topic 2)
Which of The following would offer the MOST insight with regard to an organization's risk culture?

A. Risk management procedures
B. Senior management interviews
C. Benchmark analyses
D. Risk management framework

Answer: B

NEW QUESTION 771
- (Exam Topic 2)
A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

A. Assessing the degree to which the control hinders business objectives
B. Reviewing the IT policy with the risk owner
C. Reviewing the roles and responsibilities of control process owners
D. Assessing noncompliance with control best practices

Answer: A

NEW QUESTION 775
- (Exam Topic 2)
An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner s BEST course of action?

A. Accept the risk and document contingency plans for data disruption.
B. Remove the associated risk scenario from the risk register due to avoidance.
C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
D. Validate the transfer of risk and update the register to reflect the change.

Answer: C

NEW QUESTION 778
- (Exam Topic 2)
Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

A. Recommend the IT department remove access to the cloud services.
B. Engage with the business area managers to review controls applied.
C. Escalate to the risk committee.
D. Recommend a risk assessment be conducted.

Answer: B

NEW QUESTION 781
- (Exam Topic 2)
Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

A. Provide risk management feedback to key stakeholders.
B. Collect and analyze risk data for report generation.
C. Monitor and prioritize risk data according to the heat map.
D. Engage key stakeholders in risk management practices.

Answer: D

NEW QUESTION 785
- (Exam Topic 2)
Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

A. Obtaining funding support
B. Defining the risk assessment scope
C. Selecting the risk assessment framework
D. Establishing inherent risk

Answer: B

NEW QUESTION 788
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

A. Self-assessment questionnaires completed by management
B. Review of internal audit and third-party reports
C. Management review and sign-off on system documentation
D. First-hand direct observation of the controls in operation

Answer: B

NEW QUESTION 790
- (Exam Topic 2)
The MAIN goal of the risk analysis process is to determine the:

A. potential severity of impact
B. frequency and magnitude of loss
C. control deficiencies
D. threats and vulnerabilities

Answer: B

NEW QUESTION 792
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

A. Change testing schedule
B. Impact assessment of the change
C. Change communication plan
D. User acceptance testing (UAT)

Answer: B

NEW QUESTION 795
- (Exam Topic 2)
During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's FIRST course of action?

A. Recommend risk remediation of the ineffective controls.
B. Compare the residual risk to the current risk appetite.
C. Determine the root cause of the control failures.
D. Escalate the control failures to senior management.

Answer: C

NEW QUESTION 798
- (Exam Topic 2)
An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?

A. Redesign the heat map.

B. Review the risk tolerance.
C. Perform a business impact analysis (BIA)
D. Update the risk register.

Answer: C

NEW QUESTION 799
- (Exam Topic 2)
An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

A. identifying risk scenarios.
B. determining the risk strategy.
C. calculating impact and likelihood.
D. completing the controls catalog.

Answer: A

NEW QUESTION 802
- (Exam Topic 2)
Which of the following would provide the MOST comprehensive information for updating an organization's risk register?

A. Results of the latest risk assessment
B. Results of a risk forecasting analysis
C. A review of compliance regulations
D. Findings of the most recent audit

Answer: A

NEW QUESTION 807
- (Exam Topic 2)
Who should be responsible for implementing and maintaining security controls?

A. End user
B. Internal auditor
C. Data owner
D. Data custodian

Answer: C

NEW QUESTION 811
- (Exam Topic 2)
Which of the following methods would BEST contribute to identifying obscure risk scenarios?

A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis

Answer: A

NEW QUESTION 816
- (Exam Topic 2)
Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

A. Total cost of ownership
B. Resource dependency analysis
C. Cost-benefit analysis
D. Business impact analysis

Answer: C

NEW QUESTION 821
- (Exam Topic 2)
Read" rights to application files in a controlled server environment should be approved by the:

A. business process owner.
B. database administrator.
C. chief information officer.
D. systems administrator.

Answer: A

NEW QUESTION 823
- (Exam Topic 2)

Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

A. Senior management
B. Project manager
C. Project sponsor
D. IT risk manager

Answer: A

NEW QUESTION 826
- (Exam Topic 2)
Which of the following is a KEY responsibility of the second line of defense?

A. Implementing control activities
B. Monitoring control effectiveness
C. Conducting control self-assessments
D. Owning risk scenarios

Answer: B

NEW QUESTION 829
- (Exam Topic 2)
Which of the following would BEST help secure online financial transactions from improper users?

A. Review of log-in attempts
B. Multi-level authorization
C. Periodic review of audit trails
D. Multi-factor authentication

Answer: D

NEW QUESTION 834
- (Exam Topic 2)
Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

A. Control analysis
B. Scenario analysis
C. Heat map analysis

Answer: C

NEW QUESTION 839
- (Exam Topic 2)
The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:

A. the third-party website manager
B. the business process owner
C. IT security
D. the compliance manager

Answer: B

NEW QUESTION 842
- (Exam Topic 2)
Before implementing instant messaging within an organization using a public solution, which of the following should be in place to mitigate data leakage risk?

A. A data extraction tool
B. An access control list
C. An intrusion detection system (IDS)
D. An acceptable usage policy

Answer: D

NEW QUESTION 843
- (Exam Topic 2)
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

A. Trends in IT resource usage
B. Trends in IT maintenance costs
C. Increased resource availability
D. Increased number of incidents

Answer: A

NEW QUESTION 844

- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.

Answer: D

NEW QUESTION 848
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

A. Providing oversight of risk management processes
B. Implementing processes to detect and deter fraud
C. Ensuring that risk and control assessments consider fraud
D. Monitoring the results of actions taken to mitigate fraud

Answer: B

NEW QUESTION 849
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

A. Percentage of vulnerabilities remediated within the agreed service level
B. Number of vulnerabilities identified during the period
C. Number of vulnerabilities re-opened during the period
D. Percentage of vulnerabilities escalated to senior management

Answer: A

NEW QUESTION 852
- (Exam Topic 2)
Which of the following is the BEST measure of the effectiveness of an employee deprovisioning process?

A. Number of days taken to remove access after staff separation dates
B. Number of days taken for IT to remove access after receipt of HR instructions
C. Number of termination requests processed per reporting period
D. Number of days taken for HR to provide instructions to IT after staff separation dates

Answer: A

NEW QUESTION 853
- (Exam Topic 2)
Which of the following statements BEST describes risk appetite?

A. The amount of risk an organization is willing to accept
B. The effective management of risk and internal control environments
C. Acceptable variation between risk thresholds and business objectives
D. The acceptable variation relative to the achievement of objectives

Answer: A

NEW QUESTION 858
- (Exam Topic 2)
Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?

A. Management has not determined a final implementation date.
B. Management has not completed an early mitigation milestone.
C. Management has not secured resources for mitigation activities.
D. Management has not begun the implementation.

Answer: C

NEW QUESTION 861
- (Exam Topic 2)
A risk practitioner is reporting on an increasing trend of ransomware attacks in the industry. Which of the following information is MOST important to include to enable an informed response decision by key stakeholders?

A. Methods of attack progression
B. Losses incurred by industry peers
C. Most recent antivirus scan reports
D. Potential impact of events

Answer: D

NEW QUESTION 864
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

A. the cost associated with each control.
B. historical risk assessments.
C. key risk indicators (KRIs).
D. information from the risk register.

Answer: D

NEW QUESTION 868
- (Exam Topic 2)
After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:

A. record risk scenarios in the risk register for analysis.
B. validate the risk scenarios for business applicability.
C. reduce the number of risk scenarios to a manageable set.
D. perform a risk analysis on the risk scenarios.

Answer: B

NEW QUESTION 873
- (Exam Topic 2)
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance
B. Risk appetite
C. Risk awareness
D. Risk policy

Answer: B

NEW QUESTION 877
- (Exam Topic 2)
Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

A. Prepare a report for senior management.
B. Assign responsibility and accountability for the incident.
C. Update the risk register.
D. Avoid recurrence of the incident.

Answer: D

NEW QUESTION 878
- (Exam Topic 2)
An organization is increasingly concerned about loss of sensitive data and asks the risk practitioner to assess the current risk level. Which of the following should the risk practitioner do FIRST?

A. Identify staff members who have access to the organization's sensitive data.
B. Identify locations where the organization's sensitive data is stored.
C. Identify risk scenarios and owners associated with possible data loss vectors.
D. Identify existing data loss controls and their levels of effectiveness.

Answer: D

NEW QUESTION 880
- (Exam Topic 2)
Which of the following is the BEST indication of the effectiveness of a business continuity program?

A. Business continuity tests are performed successfully and issues are addressed.
B. Business impact analyses are reviewed and updated in a timely manner.
C. Business continuity and disaster recovery plans are regularly updated.
D. Business units are familiar with the business continuity plans and process.

Answer: A

NEW QUESTION 882
- (Exam Topic 2)
Which of the following is MOST important to ensure when continuously monitoring the performance of a client-facing application?

A. Objectives are confirmed with the business owne
B. Control owners approve control changes.
C. End-user acceptance testing has been conducte
D. Performance information in the log is encrypte

Answer: B

NEW QUESTION 883
- (Exam Topic 2)
Which of the following BEST indicates effective information security incident management?

A. Monthly trend of information security-related incidents
B. Average time to identify critical information security incidents
C. Frequency of information security incident response plan testing
D. Percentage of high risk security incidents

Answer: C

NEW QUESTION 886
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?

A. Audit engagement letter
B. Risk profile
C. IT risk register
D. Change control documentation

Answer: C

NEW QUESTION 887
- (Exam Topic 2)
A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:

A. update the risk rating.
B. reevaluate inherent risk.
C. develop new risk scenarios.
D. implement additional controls.

Answer: A

NEW QUESTION 892
- (Exam Topic 2)
Prior to selecting key performance indicators (KPIs), itis MOST important to ensure:

A. trending data is available.
B. process flowcharts are current.
C. measurement objectives are defined.
D. data collection technology is available.

Answer: C

NEW QUESTION 897
- (Exam Topic 2)
Which of the following is MOST important when discussing risk within an organization?

A. Adopting a common risk taxonomy
B. Using key performance indicators (KPIs)
C. Creating a risk communication policy
D. Using key risk indicators (KRIs)

Answer: A

NEW QUESTION 902
- (Exam Topic 2)
Which of the following will BEST support management repotting on risk?

A. Risk policy requirements
B. A risk register
C. Control self-assessment
D. Key performance Indicators

Answer: B

NEW QUESTION 907
- (Exam Topic 2)
An organization is measuring the effectiveness of its change management program to reduce the number of unplanned production changes. Which of the following would be the BEST metric to determine if the program is performing as expected?

A. Decrease in the time to move changes to production
B. Ratio of emergency fixes to total changes

C. Ratio of system changes to total changes
D. Decrease in number of changes without a fallback plan

Answer: B

NEW QUESTION 909
- (Exam Topic 1)
Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

A. To build an organizational risk-aware culture
B. To continuously improve risk management processes
C. To comply with legal and regulatory requirements
D. To identify gaps in risk management practices

Answer: B

NEW QUESTION 913
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?

A. Unencrypted data
B. Lack of redundant circuits
C. Low bandwidth connections
D. Data integrity

Answer: A

NEW QUESTION 915
- (Exam Topic 1)
An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

A. Develop a compensating control.
B. Allocate remediation resources.
C. Perform a cost-benefit analysis.
D. Identify risk responses

Answer: D

NEW QUESTION 919
- (Exam Topic 1)
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

A. Identify the potential risk.
B. Monitor employee usage.
C. Assess the potential risk.
D. Develop risk awareness training.

Answer: A

NEW QUESTION 923
- (Exam Topic 1)
Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

A. Perform an m-depth code review with an expert
B. Validate functionality by running in a test environment
C. Implement a service level agreement.
D. Utilize the change management process.

Answer: C

NEW QUESTION 927
- (Exam Topic 1)
Establishing and organizational code of conduct is an example of which type of control?

A. Preventive
B. Directive
C. Detective
D. Compensating

Answer: B

NEW QUESTION 928
- (Exam Topic 1)
An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

A. Service level agreement
B. Customer service reviews
C. Scope of services provided
D. Right to audit the provider

Answer: D

NEW QUESTION 932
- (Exam Topic 1)
Which of the following should be the risk practitioner s PRIMARY focus when determining whether controls are adequate to mitigate risk?

A. Sensitivity analysis
B. Level of residual risk
C. Cost-benefit analysis
D. Risk appetite

Answer: C

NEW QUESTION 933
- (Exam Topic 1)
A contract associated with a cloud service provider MUST include:

A. ownership of responsibilities.
B. a business recovery plan.
C. provision for source code escrow.
D. the providers financial statements.

Answer: A

NEW QUESTION 938
- (Exam Topic 1)
Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

A. Obtaining logs m an easily readable format
B. Providing accurate logs m a timely manner
C. Collecting logs from the entire set of IT systems
D. implementing an automated log analysis tool

Answer: B

NEW QUESTION 941
- (Exam Topic 1)
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?

A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects

Answer: A

NEW QUESTION 943
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

* CRISC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year